California Department of Veterans Affairs

News For Veterans

Contact: J.P. Tremblay
Jerry Jones
Jaime Arteaga
Legislation and Public Affairs
916-653-2192
Fax 916-653-2611
July 19, 2006

NEWS FROM THE CALIFORNIA DEPARTMENT OF VETERANS AFFAIRS

UPDATED INFORMATION REGARDING THE THEFT OF VETERANS DATA FROM THE UNITED STATES DEPARTMENT OF VETERANS AFFAIRS

LATEST INFORMATION:

The Administration has concluded that credit monitoring services and the associated funding will no longer be necessary.

The proposal for free credit monitoring for veterans whose personal information was stolen has been withdrawn because the laptop containing their data has been recovered. The president sent a letter to Congress on July 18, 2006, canceling last month's request for $160.5 million in additional funding for the Veterans Affairs Department to provide one year of free monitoring to millions of veterans and active-duty troops. The FBI has determined with a "high degree of confidence" that information stored on the stolen laptop and external drive was not accessed or compromised.

The letter can be accessed at the following URL:

http://www.whitehouse.gov/omb/budget/amendments/supplemental8a_7_18_06.pdf

PRIOR INFORMATION:

In a *News For Veterans*, dated June 21, 2006, we provided a story from the United States Department of Veterans Affairs (USDVA), which included the following statement concerning credit monitoring:

"As part of the continuing efforts by the Department of Veterans Affairs (VA) to protect and assist those potentially affected by the recent data theft that occurred at an employee's Maryland home, Secretary of Veterans Affairs R. James Nicholson today announced that VA will provide one year of free credit monitoring to people whose sensitive personal information may have been stolen in the incident."

This story can be accessed at the following URL:
http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1143

In a *News For Veterans*, dated June 30, 2006, we provided a story from the USDVA indicating that the stolen computer and the data were recovered on June 29, 2006.

This story can be accessed at the following URL:
http://www1.va.gov/opa/data/Data_Security_Issue_Update.asp

The USDVA has recently released two Security Issue Updates.

July 14, 2006. Data Security Issue Update.

On Thursday, June 29, 2006, Veterans Affairs Secretary R. James Nicholson announced that law enforcement authorities recovered the laptop and external hard drive stolen in early May from a VA employee's home. The FBI has since informed VA that it has completed its forensic examination of the recovered laptop and hard drive. The FBI indicated to VA that it has a high degree of confidence -- based on the results of the forensic tests and other information gathered during the investigation -- that the sensitive files were not accessed or compromised.

The update can be accessed at the following URL:
http://www1.va.gov/opa/data/july14.asp

July 17, 2006. Data Security Issue Update

VA to Conduct Data Breach Analysis; Individual Credit Monitoring No Longer Necessary

Given the FBI's high degree of confidence that the information recently recovered was not accessed or compromised, VA believes that individual credit monitoring will no longer be necessary. Still, protecting veterans' private information remains a priority for VA. Out of an abundance of caution, and to further safeguard individuals' information, VA will work swiftly to solicit bids from companies that provide data breach analysis. Data breach analysis looks across multiple industries to detect patterns of misuse related to a specific data loss. While it is considered highly unlikely by the FBI and law enforcement that this data was accessed, data breach analysis will provide additional assurances. VA has funds in its budget that can be used for this purpose, and there will be no reduction in the quality of health care and other services provided to veterans as a result of this expenditure. The Secretary remains unwavering in his resolve to make VA the leader in protecting personal information, training and educating our employees in best practices, and establishing a culture that always puts the safekeeping of veterans' personal information first.

The update can be accessed at the following URL:
http://www1.va.gov/opa/data/july17.asp

_____
_____